Systems Design & Integrated System Health Management (ISHM) Technologies

Dr. Francesca A. Barrientos

Complex System Design & Engineering Group
Discovery and Systems Health Technical Area
Intelligent Systems Division
NASA Ames Research Center

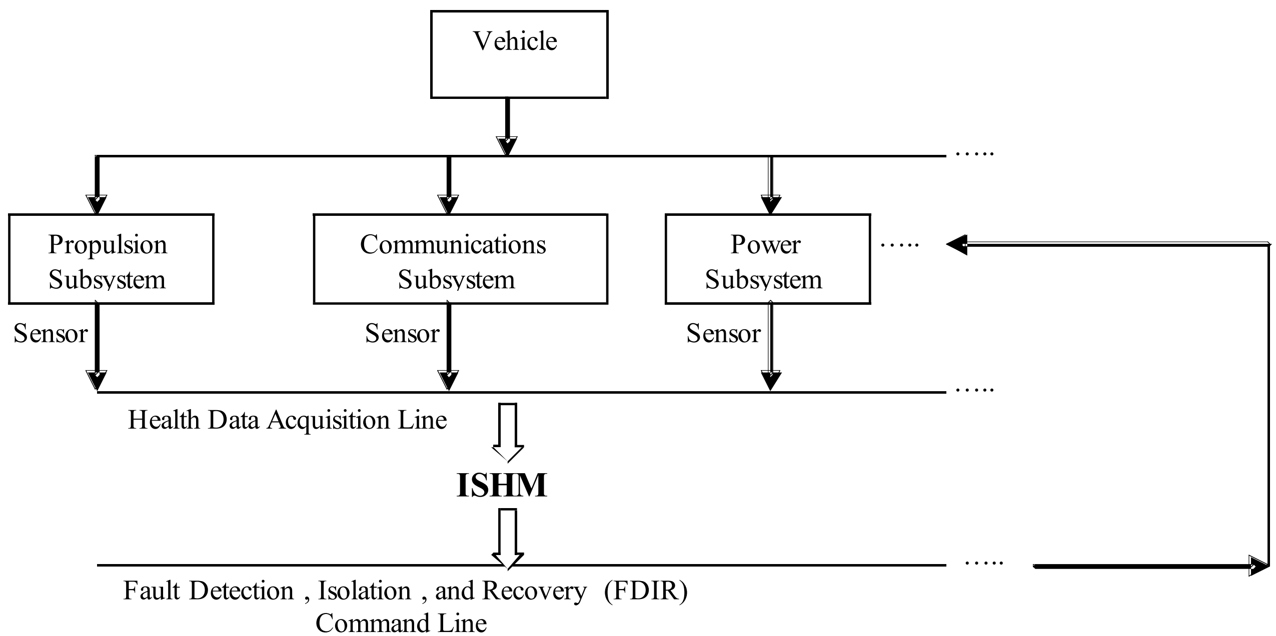
ISHM for Exploration Systems

The art and science of managing off-nominal conditions systems may encounter during their operational life either by designing out failures early on, or designing in the capability to safeguard against or mitigate failures

- Key enabler for crew self sufficiency and even autonomy
- **True ISHM has never been achieved**
- Key limitation: ISHM typically retrofitted onto *subsystems* after the vehicle has been designed or even built

ISHM Challenge for Exploration Missions

ISHM design must be part of the overall design process and viewed as a system engineering discipline, encompassing a range of technologies & methods



Facing the Challenge of ISHM Design

- Early influence on system design to guide choice of health management methods and technologies
  - Eliminate/reduce likelihood of failure by design through part selection and built-in redundancy
  - Prognosis in conjunction with preventative maintenance
  - Fault management with diagnosis and recovery technologies
- Failure modes & effects analysis activities for ISHM
  - Feed fault information into the design process to create simulations of faults and improved designs to deal with faults
- The initial design must be examined in the context of the full system life cycle
  - Include all stakeholders (ops, maintenance, etc.) in the design
  - Solution optimized in terms of well-defined Figures of Merit (FOMs)

The current state of ISHM Design

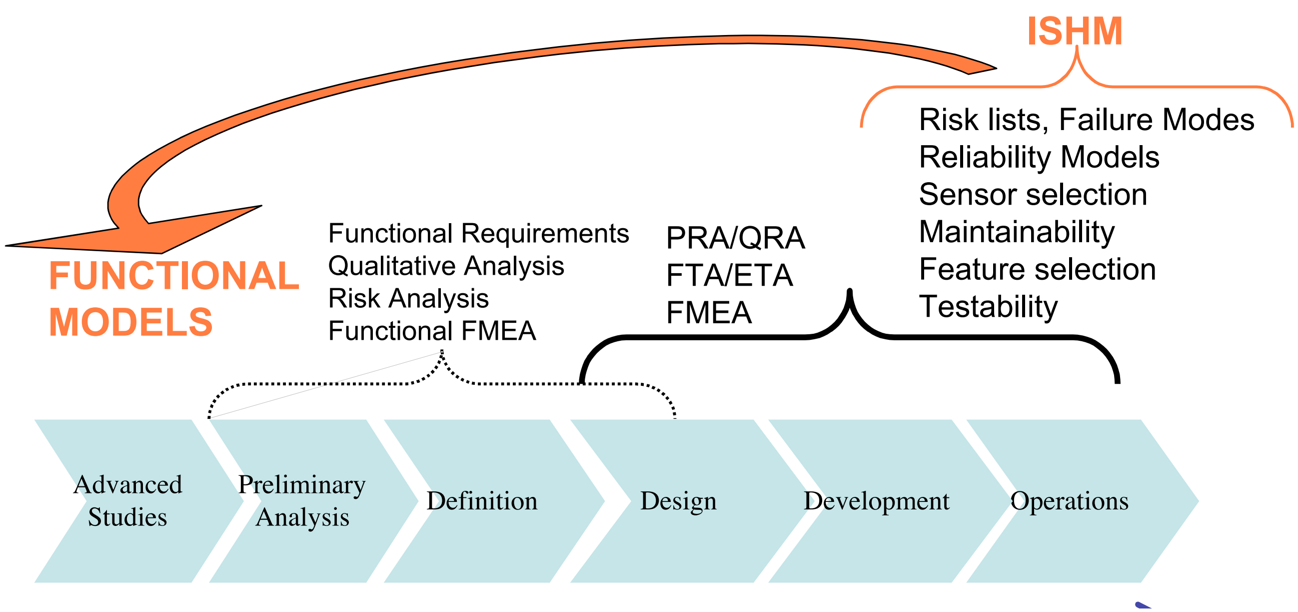
- Insufficient interaction during the design process between failure analysis activities and design processes to prevent or mitigate these failures
- Limited interaction between reliability analyses and design processes
- Little interaction between operational training simulations and assessments of operational dependability and design process
- Operations and maintenance costs and risks become much larger than initially projected during Phase A initial design
- No formal tools and methodologies to allow program managers and engineering designers to formulate a clear understanding of the impact of the decisions on the downstream phases such as operations and maintenance on the systems design, and vice versa

ISHM Design Goal

"DESIGN IN" THE ISHM CAPABILITY FROM THE BEGINNING!

- Good news: Current interest is strong!
  - First international forum on Integrated Systems Health Engineering and Management held in November
  - CEV/CLV
- Bad news: We lack methodologies & tools to achieve this!
- Some successful attempts
  - Requirements: Specify ISHM "shall" statements at beginning of project
    - Joint Strike Fighter (5% of requirements are HM related)
    - Boeing 777
    - CEV and CLV (planned)
  - Trade Studies: Integrate ISHM design with system-level design and do trade studies with ISHM as a design attribute
    - Northrop/NASA ARC SA&O effort for 2nd Gen RLV program
    - Honeywell/QSI SA&O and modeling effort
  - Integrate operations and maintenance considerations into design:
    - Boeing 777

The ISHM Design Paradigm:
Changing the Way ISHM Design is Done



Proposed Design Paradigm Shift #1: Integrate ISHM design into very early functional design stage (including failure and reliability analyses)

Proposed Design Paradigm Shift #2: Assess impact/tradeoffs of ISHM Figures of Merit (FOMs) on system level FOMs from all stakeholders throughout mission lifecycle

Key Challenges for Paradigm Shift

- Embedding ISHM design into early functional design requires high-level modeling and analyses
  - Models of system components and design parameters are not yet available
  - Integrating health management for complex systems requires capability to model functionality of individual subsystems as well as their interactions
- Conducting failure, reliability and risk analyses during functional design stage
  - Need mathematical techniques for risk assessment and resource allocation under uncertainty must be incorporated with high-level analyses
- Design of ISHM is multidisciplinary and multi-objective by nature
  - Need mathematical framework to achieve effective analysis & optimization
  - Designing an ISHM that encompasses all subsystems of a space mission is the result of interaction among engineers and managers from different disciplines with their own domain expertise

Candidate Design Methods

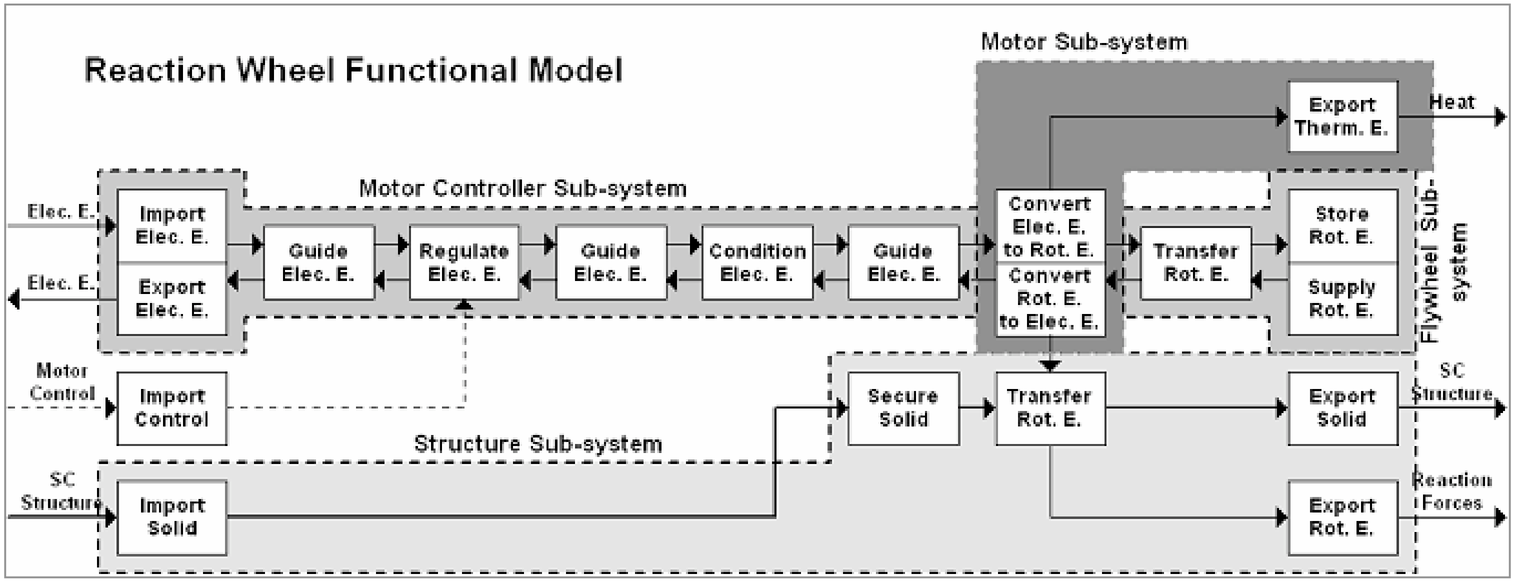
- Risk and Reliability Based Design Methods
  - PRA, FTA, FMEA/FMECA, reliability block diagrams, event sequence diagrams, safety factors, knowledge-based methods, expert elicitation
- Design for Testability Methods
- Formal design theory and methodology
  - Function-based design and modeling
  - Mathematical techniques:
    - Uncertainty modeling, decision-based design, risk-based design, design optimization, etc.
  - Design for *X* methodologies
    - Design for *ISHM*, Design for *maintainability*, Design for *failure prevention, …*

CSDE group R&D efforts

- Function-based modeling and failure analysis
- Risk assessment by portfolio management and optimization
- Multi-objective and multi-disciplinary system analysis & optimization

Function-Based Design, Modeling & Failure Modes Analysis for ISHM Design

- Develop “functional model” of vehicle and ISHM subsystems
- Standardized representation enables retrieval of design knowledge based on common functionality

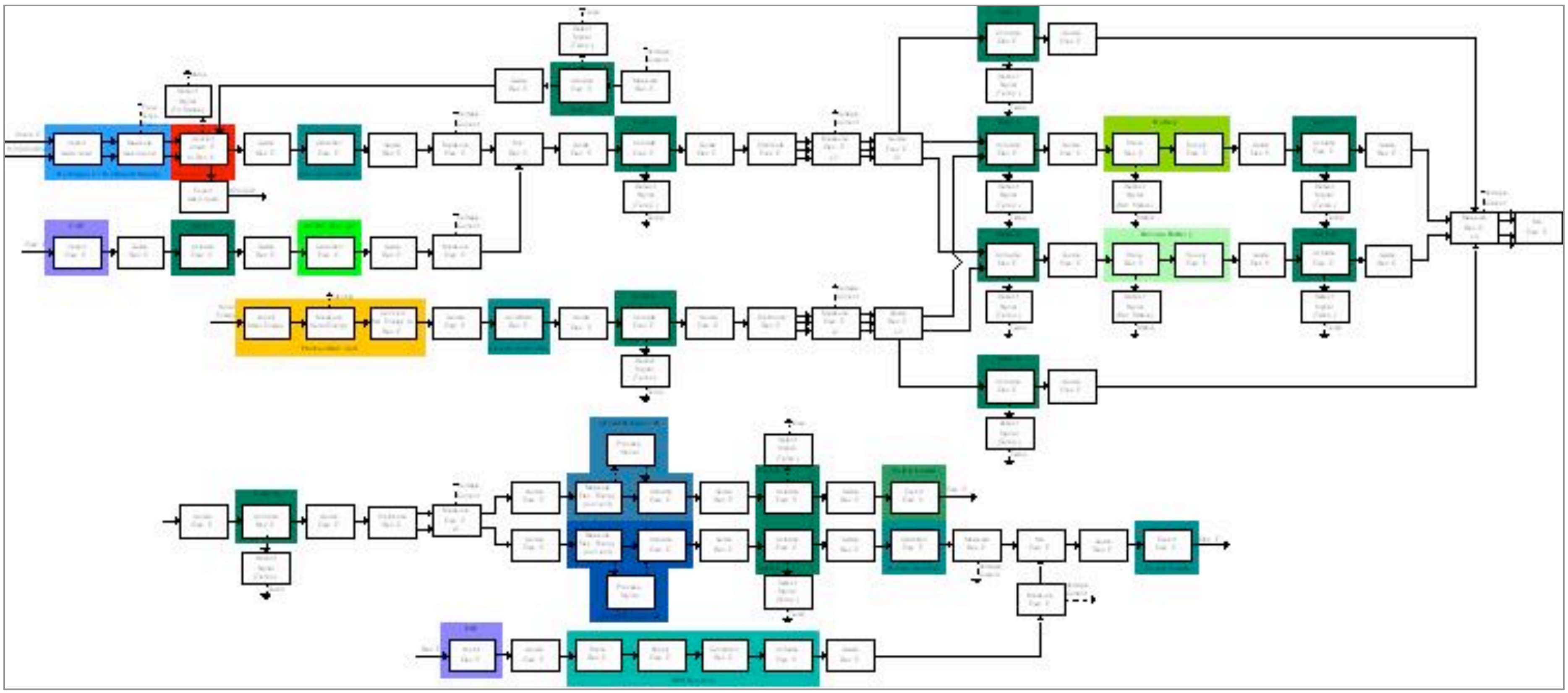


- Correlate historical and potential failure modes with functionality
- Functional model as living document during system lifecycle from design through operations

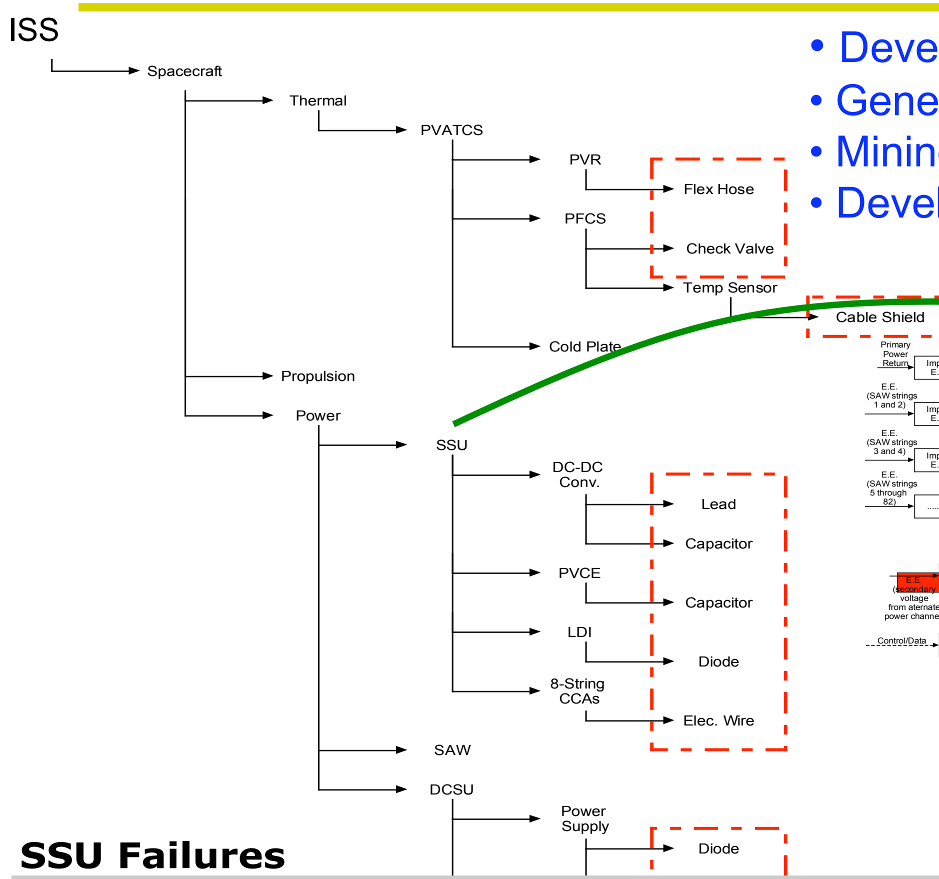
The ISHM System Functional *Blueprint*

Ex: Design of the ADAPT testbed at NASA ARC

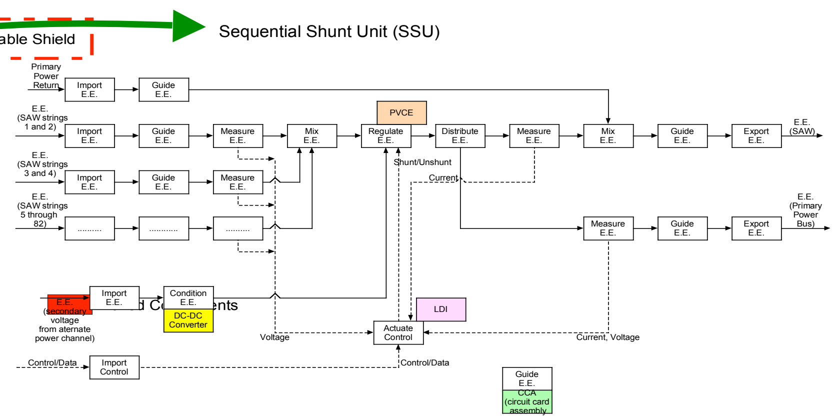
- Used to discover interfaces and interactions between functions
- Used to add required functionality for ISHM (detect, sense, activate, etc.)
- Used to discover functional failures and add safeguards



Function-Based Failure Modes Analysis



- Developing templates for functional models
- Generating database of functions for S/C
- Mining Failure Databases
- Developing a Software Query Interface

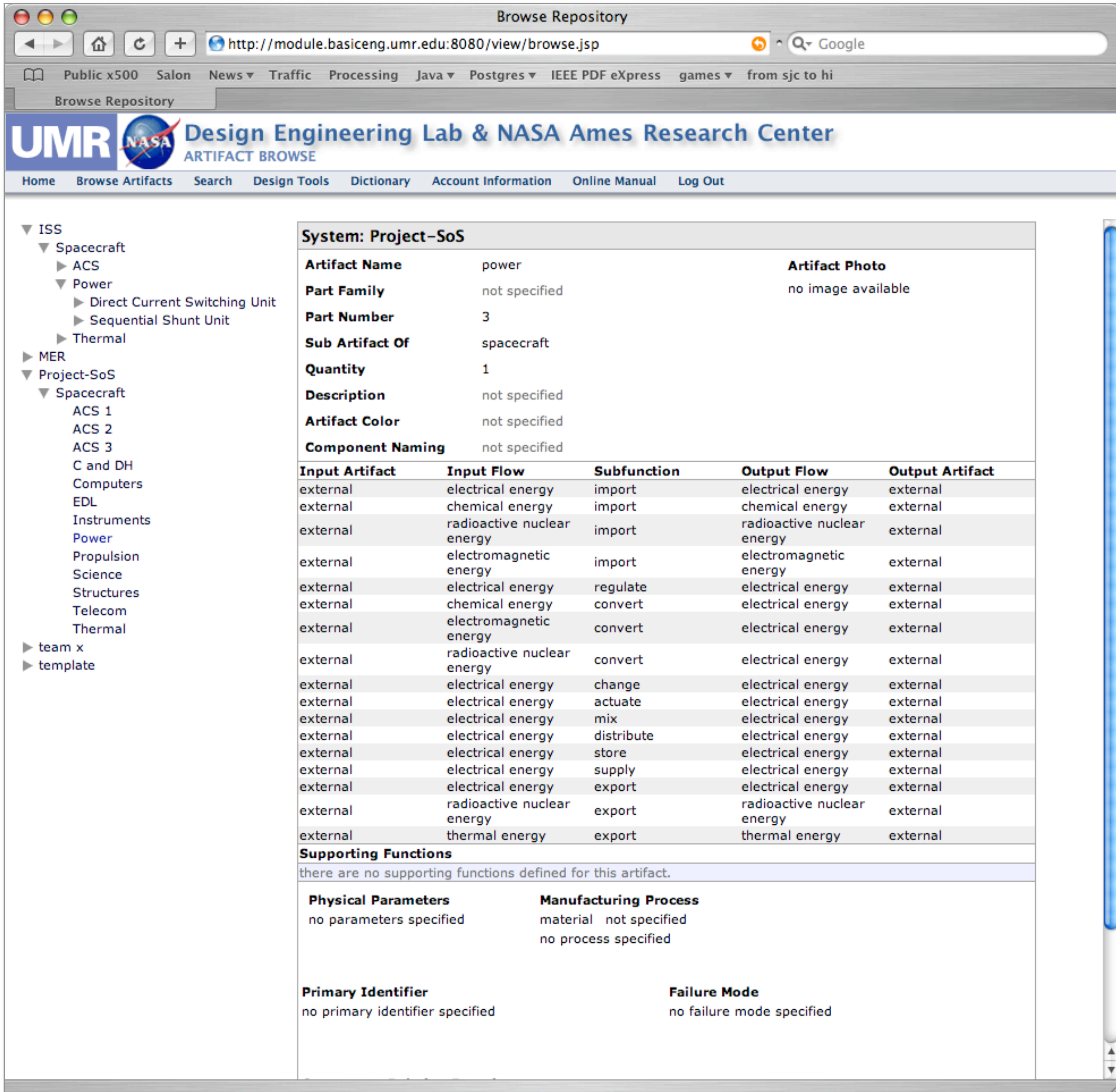


Components in colored boxes have failures identified from reports

SSU Failures

Failure Mode	Primary Identifier	Component	Subfunction	Flow	Sub-assembly
Arc Discharge	Breakdown	electric wire	Guide	electrical	8-String CCAs
	Breakdown	diode	Guide/Stop	electrical	LDI
Abrasive Wear	Wear	lead	Guide	electrical	DC-DC Converter
Arc Discharge	Breakdown	capacitor	Store/Supply	electrical	DC-DC Converter
Electrical Overstress	Overstress	capacitor	Store/Supply	electrical	PVCE

FFMEA Design Interface (w/ UMR)



Browse Repository

http://module.basiceng.umr.edu:8080/view/browse.jsp

Public x500 Salon News Traffic Processing Java Postgres IEEE PDF eXpress games from sjc to hi

Browse Repository

UMR Design Engineering Lab & NASA Ames Research Center

ARTIFACT BROWSE

Home Browse Artifacts Search Design Tools Dictionary Account Information Online Manual Log Out

- ISS
  - Spacecraft
    - ACS
    - Power
      - Direct Current Switching Unit
      - Sequential Shunt Unit
    - Thermal
- MER
- Project-SoS
  - Spacecraft
    - ACS 1
    - ACS 2
    - ACS 3
    - C and DH
    - Computers
    - EDL
    - Instruments
    - Power
    - Propulsion
    - Science
    - Structures
    - Telecom
    - Thermal
- team x
- template

System: Project-SoS

Artifact Name	power	**Artifact Photo**
Part Family	not specified	no image available
Part Number	3	
Sub Artifact Of	spacecraft	
Quantity	1	
Description	not specified	
Artifact Color	not specified	
Component Naming	not specified	

Input Artifact	Input Flow	Subfunction	Output Flow	Output Artifact
external	electrical energy	import	electrical energy	external
external	chemical energy	import	chemical energy	external
external	radioactive nuclear energy	import	radioactive nuclear energy	external
external	electromagnetic energy	import	electromagnetic energy	external
external	electrical energy	regulate	electrical energy	external
external	chemical energy	convert	electrical energy	external
external	electromagnetic energy	convert	electrical energy	external
external	radioactive nuclear energy	convert	electrical energy	external
external	electrical energy	change	electrical energy	external
external	electrical energy	actuate	electrical energy	external
external	electrical energy	mix	electrical energy	external
external	electrical energy	distribute	electrical energy	external
external	electrical energy	store	electrical energy	external
external	electrical energy	supply	electrical energy	external
external	electrical energy	export	electrical energy	external
external	radioactive nuclear energy	export	radioactive nuclear energy	external
external	thermal energy	export	thermal energy	external

Supporting Functions

there are no supporting functions defined for this artifact.

Physical Parameters
no parameters specified

Manufacturing Process
material not specified
no process specified

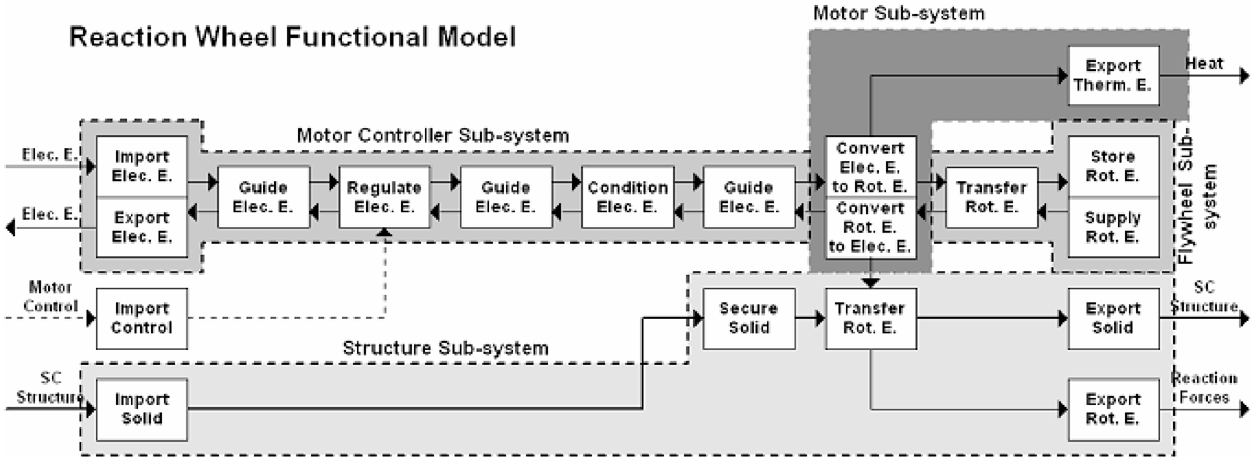
Primary Identifier
no primary identifier specified

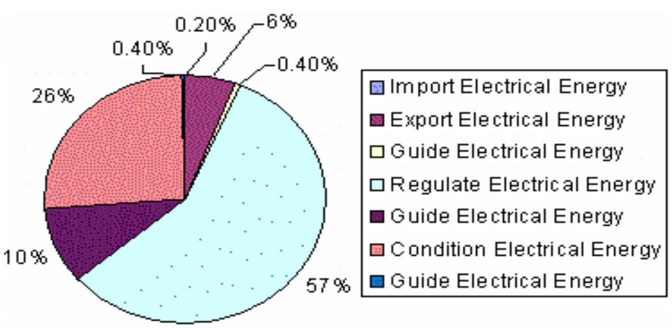
Failure Mode
no failure mode specified

Resource allocation to minimize risks due to functional failures

- **Use of formal risk-based design and optimization techniques for ISHM risk assessment**
  - Risk-informed trade study framework to account for risk & uncertainty in early design: RUBIC design
  - Framework for quantifying risk due functional failures and allocating resources for risk reduction during concurrent design
  - Starting from the functional model, RUBIC optimally allocates resources to mitigate risks due to functional failures
    - Ex of resources: hours spent on analysis, redesign, dollars allocated, acquiring more reliable components, adding redundancy, etc.

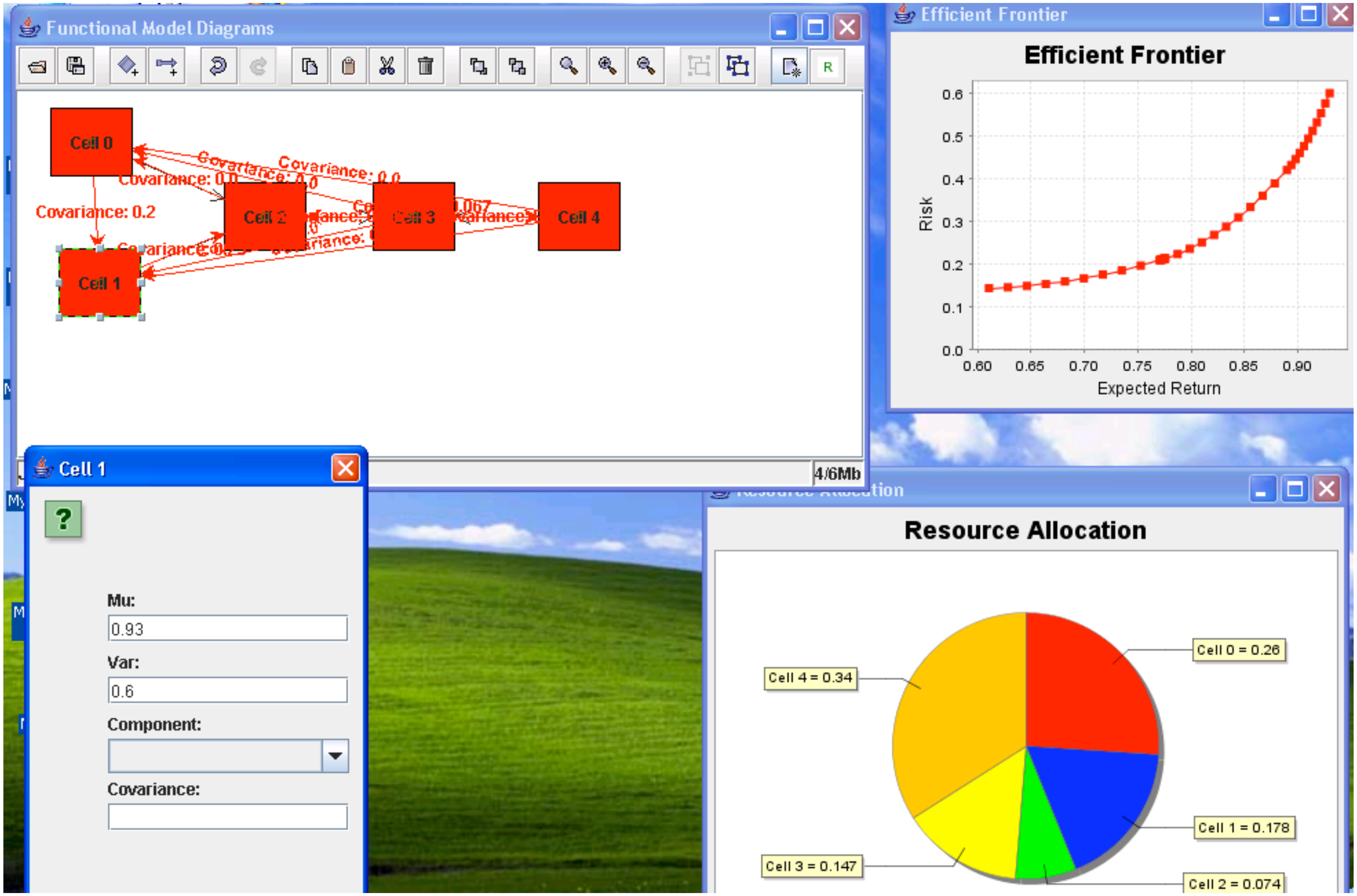
Resource Reallocation to Minimize Risk and Uncertainty due Functional Failures





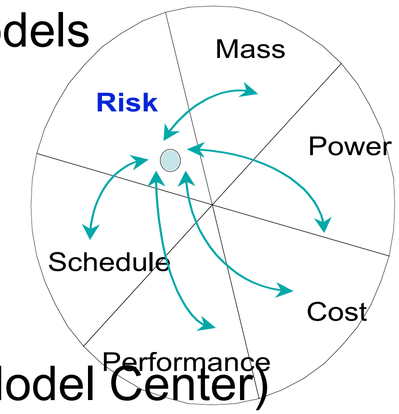
Column #	Subsystem	Function	Resource Allocation
1st	Motor Controller	Import Electrical Energy	<<1%
2nd	Motor Controller	Export Electrical Energy	4%
3rd	Motor Controller	Guide Electrical Energy	<<1%
4th	Motor Controller	Regulate Electrical Energy	36%
5th	Motor Controller	Guide Electrical Energy	6%
6th	Motor Controller	Condition Electrical Energy	17%
7th	Motor Controller	Guide Electrical Energy	<<1%
Total Allocation to Controller Subsystem: 64%			
8th	Motor Controller	Convert Electrical E. to Rotational E.	9%
2nd	Motor Controller	Convert Rotational E. to Electrical E.	13%
3rd	Motor Controller	Export Thermal Energy	10%

RUBIC Prototype Development



System Analysis & Optimization (SA&O)

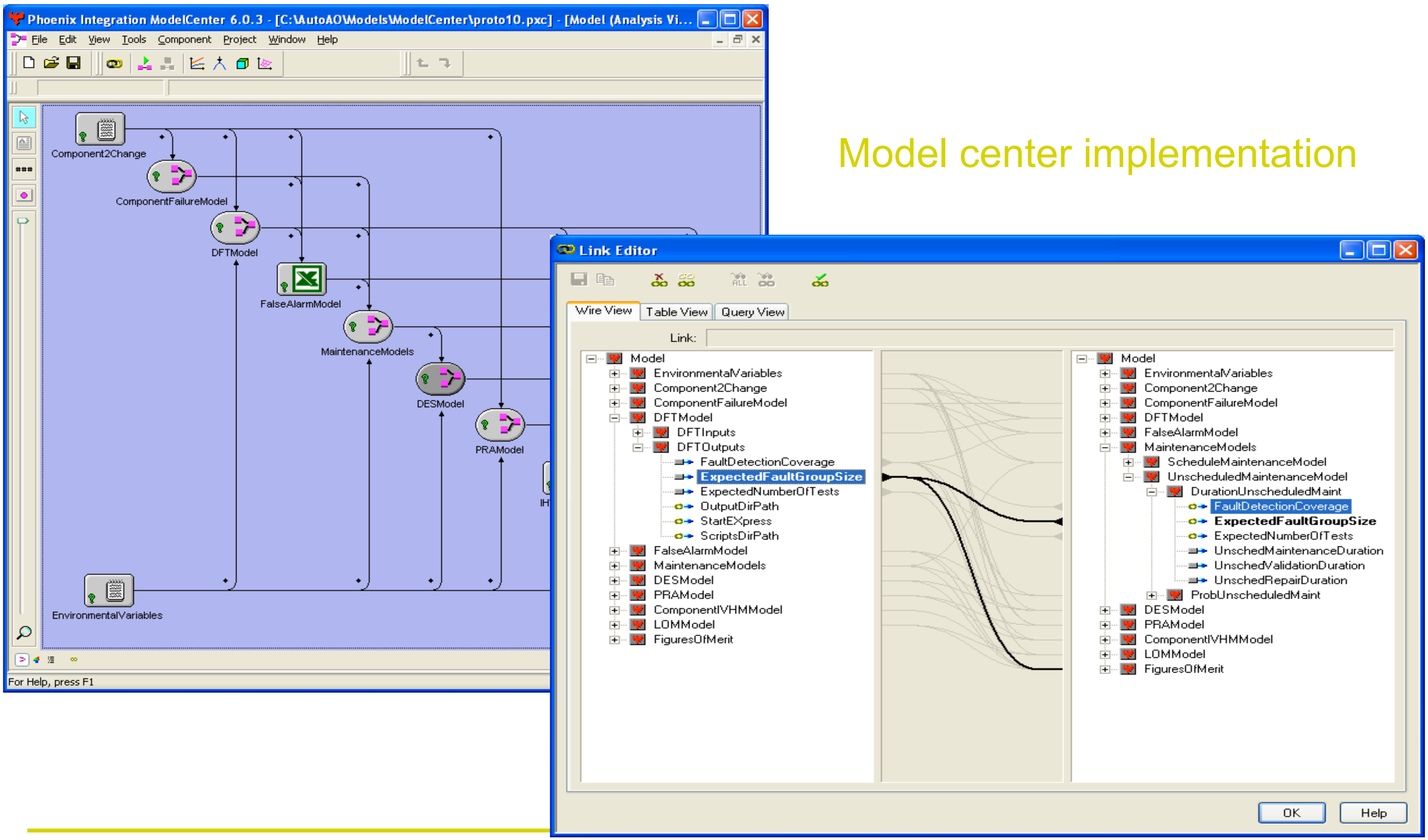
- SA&O Framework (based on prior work done for 2nd Gen RLV)
  - Select a set of Figures-of-Merit
  - Select a set of models---such as cost, safety, operations, reliability, false alarm rates and maintainability---that generate FOMs
  - Determine the tools to implement the models
  - Determine the data flow requirements between the models
  - Perform trade studies



- Current Enhancements:
  - **Multi-objective & multi-disciplinary optimization**
  - **Data flow/exchange environment** (implemented in Model Center)
  - **Automation for rapid trade analyses**
  - Ability to feed back into functional design stage:
    - Add new functionality to enable ISHM to operate as an integrated system?
    - Change functionality to enable maintainability, performance, reduce risk?

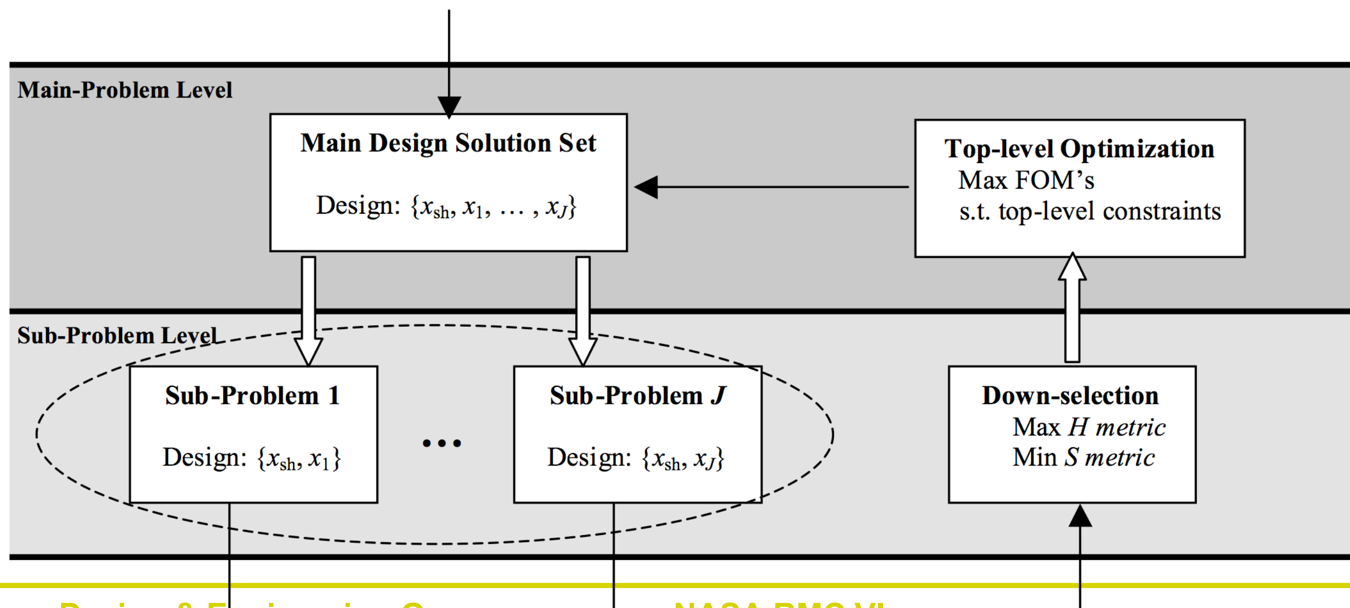
ISHM System Analysis & Optimization

Model center implementation



Multi-Disciplinary, Multi-Objective Optimization for ISHM Design

- ISHM design can be formulated as an optimization problem
  - ISHM Design Variables
  - ISHM Objectives (Figures of Merit)
  - ISHM Design Constraints: Feasibility Constraints + Hard Requirements
- Multi-objectives/constraints in each sub-system
  - Functionally separable $F_{i,j}$ and exclusive f_j
  - S Metric to encourage convergence; H Metric to encourage diversity



Summary & Conclusions

- ISHM is a key enabler for exploration systems
- Towards ISHM as a systems engineering discipline and co-design with vehicle systems
- Complex System Design & Engineering Group Research
  - Function based failure modes analysis
  - Risk and uncertainty based design
  - ISHM system analysis and optimization (SA&O)
  - Current Involvement:
    - CEV, CLV for Constellation/ESMD
    - IVHM and Aging Aircraft for Aviation Safety/ARMD

An ISHM design paradigm shift is required for a successful and sustainable exploration endeavor

Questions, Comments, Suggestions

Complex Systems Design & Engineering Group

Intelligent Systems Division, NASA ARC

Francesca Barrientos

francesca.a.barrientos@nasa.gov

Irem Tumer, Group lead

irem.y.tumer@nasa.gov